Legal Aspects of Cyberspace Operations AusCERT 2012

Agenda

- Cyberspace Operations
  - Computer Network Security & Defense
  - Computer Network Exploitation
  - Computer Network Terrorism
  - Computer Network Attack
- Case Studies
  - Stuxnet
  - Georgia
  - Estonia

Disclaimer

Disclaimer - aka the fine print

- Joint Ethics Regulation
- Views are those of the speaker
- I'm here in personal capacity
- Don't represent view of government
- Disclaimer required at beginning of presentation.

All material - unclassified

Court Recognizes Your Special Skills

- ***United States v. Prochner,* 417 F.3d 54 (D. Mass. July 22, 2005)**
  - **Definition of Special Skills**
    - **Special skill - a skill not possessed by members of the general public and usually requiring substantial education, training or licensing.**
      - **Examples - pilots, lawyers, doctors, accountants, chemists, and demolition experts**
    - **Not necessarily have formal education or training**
      - **Acquired through experience or self-tutelage**
    - **Critical question is - whether the skill set elevates to a level of knowledge and proficiency that eclipses that possessed by the general public.**

Computer Network Security & Defense

- **Common Law**
  - **Trespass to Chattel**
  - **Statutory Law**

Authority for Computer Network Security

- Common Law Doctrine-Trespass to Chattel
- Owner of personal property has a cause of action for trespass and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use
- One may use reasonable force to protect his possession against even harmless interference
- The law favors prevention over post-trespass recovery, as it is permissible to use reasonable force to retain possession of a chattel but not to recover it after possession has been lost
  - *Intel v. Hamidi,* 71 P.3d 296 (Cal. Sp. Ct. June 30, 2003

Authority for Computer Network Security

- Right to exclude people from one's personal property is not unlimited.
- Self defense of personal property one must prove that he was in a place he had a right to be, that he acted without fault and that he used reasonable force which he reasonably believed was necessary to immediately prevent or terminate the other person's trespass or interference with property lawfully in his possession
  - *Moore v. State*, 634 N.E.2d 825 (Ind. App. 1994) *and Pointer v.* State, 585 N.E. 2d 33, 36 (Ind. App. 1992)

Computer Network Security & Defense

- Privacy and Civil Liberties
  - Log-on banners and user agreements
  - Workplace policies and rules of behavior
  - Computer training

Computer Network Security & Defense

- Consent
  - Where there is a legitimate expectation of privacy, consent provides an exception to the warrant and probable cause requirement.
  - A computer log-on banner, workplace policy, or user agreement may constitute user consent to a search. *See United States v. Monroe*, 52 M.J. 326, 330 (C.A.A.F. 1999) (log-on banner stating "users logging on to this system consent to monitoring).
  - In the context of public employment, employee consent is valid only if it is limited to consent to reasonable searches. Thus, the underlying search still must be reasonable.

Computer Network Security & Defense

- **Wiretap Statute: Rights or Property Exception**
- **18 U.S.C. § 2511(2)(a)(i)**
  - **A provider "may intercept or disclose communications on its own machines "in the normal course of employment while engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider of that service."**
  - **Generally speaking, the rights or property exception allows tailored monitoring necessary to protect computer system from harm. *See U.S. v McLaren*, 957 F. Supp 215, 219 (M.D. Fla. 1997).**

Computer Network Exploitation

- **Espionage**
  - **The practice of using spies to collect information about what another government or company is doing or plans to do.**
    - **Black's Law Dictionary 585 (9th ed. 2009)**

Computer Network Exploitation

- **Roger D. Scott, *Territorial Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217 (1999)**
  - **Issue – under operational law is surreptitious spying in another nation's territory illegal?**
  - **Facts –**
    - **No sabotage or other destructive acts**
    - **simply the collection of information**
    - **through various surreptitious, intrusive means**
    - **inside a foreign nation's territory**
    - **without that nation's knowledge or consent.**

Computer Network Exploitation

- **Roger D. Scott, *Territorial Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217 (1999)**
  - **Traditional doctrinal view – spying in another's territory during peacetime is an unlawful intervention.**
    - **Lack of respect for –**
      - **Territorial boundaries of another sovereign**
        - **National airspace**
        - **Internal waters**
        - **Territorial seas.**

Computer Network Exploitation

- **Roger D. Scott, *Territorial Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217 (1999)**
  - **Espionage may give rise to the use of force as well as a response under domestic criminal law.**
  - **Espionage by ships, submarines, or aircraft raise issues of national self-defense**
    - **Shoot down of U-2s over China and former Soviet Union**
    - **North Korean attack upon the U.S.S. Pueblo**
    - **Swedish government's use of depth-charges against Soviet submarines in Sweden's territorial sea**

Computer Network Exploitation

- **The lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine called "*tu quoque*" (roughly, a nation has no standing to complain about a practice in which it itself engages). Whatever the reasons, the international legal system generally imposes no sanctions upon nations for acts of espionage except for the political costs of public denunciation, which don't seem very onerous.**

Computer Network Exploitation

- Computer Network Exploitation
  - Typically no presence inside another's territory
  - Highly unlikely that the notions of "electronic presence" or "virtual presence" will ever find their way into the law of war concept of spying
    - not physically behind enemy lines
    - no issue of acting under false pretenses by abusing protected civilian status or by wearing the enemy's uniform.

What is Cyber-Terrorism?

- What would an act of cyber-terrorism look like?
- Do we know?
- Will we find out?
- Stuxnet??

Developing a Definition of Cyber-terrorism

- By adapting the definition of domestic terrorism that was created in 18 U.S.C. 2331 we can derive a working definition of "cyber-terrorism."
- In conventional terrorism cases, the difference between a homicide or an assault and terrorism is the motive or purpose of the attack.
- Similarly, what distinguishes cyber-terrorism acts from normal intrusion cases is largely the purpose for the attack. While this is theoretically what sets terrorism apart from other violent crime, you'll see that many of the federal statutes often don't explicitly refer to motive.

Developing a Definition of Cyber-terrorism

- Based on 18 U.S.C. 2331:
  - An act involving use of a computer;
  - That is dangerous to human life;
  - That is intended to:
    - intimidate or coerce a civilian population; or
    - influence the policy of a government by coercion or intimidation
- the Department of Defense doctrinal definition, which defines terrorism as "the calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological," and insurgency as "an organized resistance movement that uses subversion, sabotage, and armed conflict to achieve its aims. Insurgencies normally seek to overthrow the existing social order and reallocate power within the country.

Terrorism

- When is a cyberattack considered cyberterrorism
- Two views for defining the term cyberterrorism:
  - **Effects-based**. Cyberterrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals other than terrorists.
  - **Intent-based**. Cyberterrorism exists when unlawful, politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage

The Law of Armed Conflict

- Is a computer network attack an act of war?
- **Obsolete concept** not mentioned in the UN Charter and seldom heard in modern diplomatic discourse.
- An **act of war** is a **violation** of another **nation's rights** under international law that is so egregious that the victim would be justified in declaring war.
- **Declarations of war** have fallen into **disuse**

The Law of Armed Conflict

- Developed to govern a regime for peacetime and conflict spectrum
- United Nations Article 2 (4) "refrain in their international relations from the threat or use of force
  - 2 exemptions –
    - security council authorizes use of force
    - self-defense
- Article 51 of the Charter provides:

Nothing in the present Chapter shall impair the inherent right of individual or collective self defense if an armed attack occurs

The Law of Armed Conflict

- unauthorized intrusion into an unclassified information system, without more, constitutes an armed attack.
- a coordinated computer network attack shuts down a nation's air traffic control system
  - along with its banking
  - financial systems
  - public utilities
  - opens the floodgates of several dams resulting in general flooding
  - causes widespread civilian deaths and property damage
- unclassified military logistics systems
  - corrupting the data in computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies
  - interfere with ability to conduct military operations

The Law of Armed Conflict

- Nondestructive insertion of a cyber capability into the computer system of another nation
  - use of force
  - an armed attack.
- Such activities—without an accompanying intent for imminent action—would not be uses of force, so long as the cyber capability lies dormant
  - Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly (Spring 2011)

The Law of Armed Conflict

- In interpreting self-defense under Article 51, cyber strategists should keep in mind that the UN Charter governs relations between nation-states, not individuals. The DoD general counsel opines that when "individuals carry out malicious [cyber] acts for private purposes, the aggrieved state does not generally have the right to use force in self-defense." To do so ordinarily requires some indicia of effective state control of the cyber actors to impute state responsibility
  - Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly (Spring 2011)